UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

TINA POWELL, individually and on behalf of all others similarly situated, Plaintiff, v. AT&T INC., Defendant.	Civil Action No. **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff TINA POWELL ("Plaintiff") brings this class action against Defendant AT&T Inc. ("AT&T" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges as follows upon information and belief:

I. INTRODUCTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from Defendant's failure to implement reasonable and industry standard data security practices.

2. AT&T, one of the nation's telecommunications giants, provides cellular services and internet to both businesses and individual customers.

3. AT&T is well aware of the life-altering impact a data breach can have on the average AT&T customer.

4. Plaintiffs and class members purchased cellular phones and/or internet services from AT&T.

5. Plaintiff brings this Complaint against Defendant for its failure to properly secure and safeguard the sensitive information that it collected and maintained as part of its regular business practices, including, but not limited to: names, usernames, password information, contact information,

dates of birth, secret questions and answers, and Social Security numbers ("Personal Identifying Information" or "PII").

6. Former and current AT&T customers are required to entrust Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities, in order to obtain products and/or services from AT&T. Defendant retains this information for at least many years and even after the relationship has ended.

7. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

8. In April 2024, AT&T became aware of a catastrophic, widespread data breach of phone records from nearly all of its customers. According to the New York Times, "the compromised data included files containing AT&T records of calls and texts from more than 100 million cellular customers, wireless network customers and landline customers from May 2022 through October 2022, and records from Jan. 2, 2023, for a small number of customers."[1] The records expose the telephone numbers which the Defendant's customer interacted with, and some cases the "user's location in the form of cell site ID numbers."[2]

9. On July 12th, 2024, Defendant explained to the public that the sensitive information had been "illegally downloaded from our workspace on a third-party cloud platform" and that an investigation has been launched alongside cybersecurity experts to understand the "nature and scope

[1] AT&T Says Phone Data of 'Nearly All' Customers Was Breached in 2022 - The New York Times (nytimes.com)

[2] Are You an AT&T Customer? Here's What to Know About the Data Breach. - The New York Times (nytimes.com)

of the criminal activity."[3]

10. This most recent breach comes just months after another data breach from the Defendant, in which "approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders"[4] had personal information leaked including the "person's full name, email address, mailing address, phone number, Social Security number, date of birth, AT&T account number and passcode."

11. Defendant failed to adequately protect Plaintiff's and Class Members' PII to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

12. In breaching its duties to properly safeguard AT&T's customers' PII and give customers timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

13. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

[3] AT&T Addresses Illegal Download of Customer Data (att.com)

[4] AT&T Addresses Recent Data Set Released on the Dark Web (att.com)

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by its IT vendors to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continued interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

15. Plaintiff and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach (*i.e.*, the breach caused monies to be charged to Plaintiff using compromised data); (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

16. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect AT&T's customers' PII from a foreseeable and preventable cyber-attack.

17. Plaintiff seeks to remedy these harms and prevent any future data compromise on

behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

II. JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant.

19. This Court has personal jurisdiction over Defendant because AT&T's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

20. Venue is proper under 18 U.S.C § 1391(b)(1) because AT&T's principal place of business is in this District and the acts and omissions giving rise to Plaintiff' claims occurred in and emanated from this District.

III. PARTIES

21. Plaintiff TINA POWELL is a citizen of Tennessee and resides in Lyles, Tennessee.

22. Defendant AT&T's principal place of business is located at 208 S. Akard St., Dallas, TX 75202.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business.

23. AT&T is a Dallas based telecom company that provides phone and internet services nationwide to customers that allows for the transfer of confidential consumer information.

24. Plaintiff and Class Members are current and former customers at AT&T.

25. The information held by Defendant or those of its vendors at the time of the Data

Breach included the unencrypted PII of Plaintiff and Class Members.

26. Upon information and belief, in the course of collecting PII from AT&T's customers, including Plaintiff, AT&T promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

27. Plaintiff and the Class Members, as former and current customers of AT&T, relied on AT&T to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

28. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

29. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Moreover, AT&T had a duty to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep its customers' PII safe and confidential.

30. Defendant had obligations created by contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

31. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class

Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

B. The Data Breach.

33. On or about July 12th 2024, AT&T released a statement about the Data Breach, informing its customers that:[5]

> **What Happened?** We learned that AT&T customer data was illegally downloaded from our workspace on a third-party cloud platform. We started an investigation and engaged leading cybersecurity experts to help us determine the nature and scope of the issue. We have confirmed the access point has been secured.
>
> Our investigation found that the downloaded data included phone call and text message records of nearly all of AT&T cellular customers from May 1, 2022 to October 31, 2022 as well as on January 2, 2023. These records identify other phone numbers that an AT&T wireless number interacted with during this time, including AT&T landline (home phone) customers. For subset of the records, one or more cell site ID numbers associated with the interactions are also included.
>
> At this time, we do not believe the data is publicly available. We continue to work with law enforcement in their efforts to arrest those involved. Based on information available to use, we understand that at least one person has been apprehended.
>
> **Data that was involved**
> The call and text records identify the phone numbers with which an AT&T number interacted during this period, including AT&T landline (home phone) customers. It also included counts of those calls or texts and total call durations for specific dates or months.
>
> We'll notify current and former customers if their information was involved.

34. Omitted from the Notice Letter were the details about the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class

[5] Unlawful Access of Customer Data - AT&T Bill & account Customer Support (att.com)

Members, who retain a vested interest in ensuring that their PII remains protected.

35. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

36. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, AT&T failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

37. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted PII of Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

C. Data Breaches Are Preventable.

38. Defendant could have prevented this Data Breach by properly securing and encrypting materials and file servers containing the PII of Plaintiff and Class Members or by AT&T exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

39. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

40. The unencrypted PII of Class Members may end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members.

41. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[6]

42. To prevent and detect data breaches Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

[6] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[7]

43. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks.

D. Defendant Knew, or Should Have Known, of the Risk Because Telecom Companies In Possession of PII Are Particularly Susceptible To Cyber Attacks.

44. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting telecom companies that collect and store PII, like Defendant, preceding the date of the breach.

45. Data breaches, including those perpetrated against companies that store PII in their systems, have become widespread.

46. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[8]

47. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records,

[7] *Id.* at 3-4.

[8] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/

May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

48. Additionally, as companies became more dependent on electronic systems to run their business,[10] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[11]

49. Defendant knew and understood that unprotected or exposed PII in the custody of telecom companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

50. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

[9]https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?

[10] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[11] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

51. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

52. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

53. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe.

54. As a telecom company in custody of AT&T's customers' PII, Defendant knew, or should have known, the importance of safeguarding PII entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security system was breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

E. Value of Personally Identifying Information

55. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12]

56. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[13] For example, Personal Information can be sold at a price ranging from $40 to $200.[14]

---

[12] 17 C.F.R. § 248.201 (2013)

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark- web-how-much-it-costs/

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available*

Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

57. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

58. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

F. Defendant Failed To Comply With FTC Guidelines

59. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

60. The guidelines also recommend that businesses use an intrusion detection system to

---

at: https://www.experian.com/blogs/ask-experian/heres-how-much-your- personal-information-is-selling-for-on-the-dark-web/

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf

expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[17]

61. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. These FTC enforcement actions include actions against telecom companies, like Defendant.

64. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

65. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices, and AT&T failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendant's failure to employ reasonable and appropriate measures to protect

[17] *Id.*

against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

66. Upon information and belief, Defendant was at all times fully aware of its obligations to protect the PII of AT&T's customers, Defendant was also aware of the significant repercussions that may result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

G. Defendant Failed To Comply With Industry Standards

67. As noted above, experts studying cyber security routinely identify telecom companies in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

68. Several best practices have been identified that a minimum should be implemented by telecom companies in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

69. Other best cybersecurity practices that are standard in the telecom industries include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

70. Upon information and belief, Defendant failed to comply with accepted standards,

thereby opening the door to the threat actor and causing the Data Breach.

H. Common Injuries & Damages

71. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant failed to undertake appropriate and adequate measures to protect the PII.

I. Data Breaches Increase Victims' Risk of Identity Theft

72. The unencrypted PII of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

73. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

74. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes, discussed below.

75. Plaintiff's and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

76. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[18]

77. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

78. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

79. The existence and prevalence of "Fullz" packages means that the PII stolen from the

[18] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sept. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas- life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground- stolen-from-texas-life-insurance-finn/

data breach can easily be linked to the unregulated data (like insurance information) of Plaintiff and the other Class Members.

80. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

81. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

J. Loss of Time to Mitigate Risk of Identity Theft & Fraud

82. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

83. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach.

84. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[19]

85. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a

[19] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[20]

86. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

K. Diminution of Value of PII

87. PII is a valuable property right.[21] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

88. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[22]

89. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[23]

90. In fact, the data marketplace is so sophisticated that consumers can actually sell their

---

[20] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

[21] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

[22] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4

[23] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[24, 25]

91. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[26]

92. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

93. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

94. The fraudulent activity resulting from the Data Breach may not come to light for many years.

95. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

---

[24] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[25] https://datacoup.com/

[26] https://digi.me/what-is-digime/

96. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to more than thirty-five million individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

97. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

L. Loss of Benefit of the Bargain

98. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay AT&T for products and/or services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect their PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with AT&T.

M. Plaintiff's Experience

99. Plaintiff TINA POWELL is a citizen of Lyles, Tennessee and has been a customer of Defendant AT&T at all relevant times. As a result of AT&T's data breach, the Named Plaintiff has incurred out of pocket costs in addition to having her phone and other personal data, and related PII, obtained by unauthorized third parties. Due to the breach, the Named Plaintiff has had to modify her email address to a different vendor, change passwords, and has had at least two unauthorized charges to her financial account(s) and other out of pocket charges. Named Plaintiff TINA POWELL has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source and would not have entrusted her PII to Defendant had she known of Defendants' lax data

security policies. Named Plaintiff TINA POWELL has a continuing interest in ensuring that her PII is protected and safeguarded from future breaches.

100. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant failed to undertake appropriate and adequate measures to protect the PII.

101. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

102. This imminent risk of future harm has materialized. Plaintiff, and many other members of the Class, have had actual harm inflicted upon their financial status, creditworthiness, and privacy, in addition to other forms of financial harm that has forced Plaintiff, and many other Class members, to incur financial loss as a downstream result of Defendant's misconduct.

103. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

104. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ACTION ALLEGATIONS

105. Plaintiff bring this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

106. Plaintiff seeks to represent the following nationwide "Economic Loss Class" as follows:

> All AT&T customers in the United States who have incurred out-of-pocket costs as a result of the Data Breach, including, but not limited to: loss of monies, unauthorized financial charges or deductions to financial accounts, or purchases of credit reports or identity theft/credit protection.

107. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

108. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

109. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. The Class is apparently identifiable within Defendant's records.

110. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

111. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

112. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges

on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

113. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

114. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

115. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a

common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

116. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

117. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

118. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

119. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a classwide basis.

120. This case is appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

VI. CLAIMS FOR RELIEF

COUNT I
Negligence

121. Plaintiff re-alleges and incorporates by reference all of the allegations contained in the

preceding paragraphs as if fully set forth herein.

122. Defendant requires AT&T's customers, including Plaintiff and Class Members, to submit non-public PII to Defendant in the ordinary course of providing its services.

123. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to its customers and clients, which solicitations and services affect commerce.

124. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

125. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

126. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its property—and Class Members' PII held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach. AT&T's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

127. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

128. Defendant owed a duty of care to Plaintiff and Class Members to provide data

security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the PII.

129. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of being customers at AT&T.

130. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

131. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

132. Defendant also had a duty to exercise appropriate clearinghouse practices to remove AT&T's former customers' PII it was no longer required to retain pursuant to regulations.

133. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

134. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

135. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove AT&T's former customers' PII it was no longer required to retain pursuant to regulations;

f. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices; and

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope so Class Members could take appropriate steps to mitigate the potential for identity theft and other damages.

136. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

137. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

138. Defendant's violations of Section 5 of the FTC Act constitute negligence.

139. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

140. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

141. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the telecom industry.

142. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

143. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems or transmitted through third party systems.

144. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

145. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

146. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

147. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

148. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost

and disclosed to unauthorized third persons as a result of the Data Breach.

149. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

150. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

151. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant failed to undertake appropriate and adequate measures to protect the PII.

152. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

153. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

154. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*

155. Plaintiff re-alleges and incorporates by reference all of the allegations contained in the preceding paragraphs as if fully set forth herein.

156. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate electronic systems and data security practices to safeguard Plaintiff' and Class Members' PII.

157. Defendant breached its duties to Plaintiff and Class Members under the FTCA by failing to provide fair, reasonable, or adequate electronic systems and data security practices to safeguard Plaintiff's and Class Members' PII.

158. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

159. Plaintiff and Class Members are within the class of persons that the FTCA intended to protect and the harm to Plaintiff and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

160. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

161. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that by failing to meet its duties, Defendant's breach would cause Plaintiff and Class Members to

experience the foreseeable harms associated with the exposure of their PII.

162. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract

163. Plaintiff re-alleges and incorporates by reference all of the allegations contained in the preceding paragraphs as if fully set forth herein. Plaintiff brings this claim against solely against Defendant.

164. Plaintiff and Class Members were required to provide their PII to AT&T as a condition of receiving products and/or services.

165. Plaintiff and the Class entrusted their PII to AT&T. In so doing, Plaintiff and the Classes entered into implied contracts with AT&T by which AT&T agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

166. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that AT&T's data security practices complied with relevant laws and regulations and were consistent with industry standards.

167. Implicit in the agreement between Plaintiff and Class Members and the AT&T to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such

information secure and confidential.

168. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and AT&T, on the other, is demonstrated by their conduct and course of dealing.

169. AT&T solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of AT&T's regular business practices. Plaintiff and Class Members accepted AT&T's offers and provided their PII to AT&T.

170. In accepting the PII of Plaintiff and Class Members, AT&T understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

171. On information and belief, at all relevant times AT&T promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

172. On information and belief, AT&T further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

173. Plaintiff and Class Members paid money to AT&T with the reasonable belief and expectation that AT&T would use part of its earnings to obtain adequate data security. AT&T failed to do so.

174. Plaintiff and Class Members would not have entrusted their PII to AT&T in the absence of the implied contract between them and AT&T to keep their information reasonably secure.

175. Plaintiff and Class Members would not have entrusted their PII to AT&T in the absence of its implied promise to monitor its electronic systems and networks to ensure that it adopted reasonable data security measures.

176. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with AT&T.

177. AT&T breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

178. As a direct and proximate result of AT&T's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

179. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

180. Plaintiff and Class Members are also entitled to injunctive relief requiring AT&T to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
Unjust Enrichment

181. Plaintiff re-alleges and incorporates by reference all of the allegations contained in the preceding paragraphs as if fully set forth herein.

182. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

183. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid money to AT&T for products and/or services as well as provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received the services that were the subject of the transaction and had their PII protected with adequate data security.

184. Defendant knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to it.

Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

185. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

186. Defendant acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

187. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendant or obtained products and/or services at AT&T.

188. Plaintiff and Class Members have no adequate remedy at law.

189. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

190. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

191. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages

from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

192. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grants the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xviii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: July 30, 2024

Respectfully submitted,

/s/ Warren T. Burns

Warren T. Burns (TX Bar No. 24053119)
Daniel H. Charest (TX Bar No. 24057803)
Hannah M. Crowe (TX Bar No. 24131156)
BURNS CHAREST LLP
900 Jackson Street, Suite 500
Dallas, TX 75202
Telephone: (469) 904-4551
Fax: (469) 444-5002
wburns@burnscharest.com
dcharest@burnscharest.com

hcrowe@burnscharest.com

Korey A. Nelson *(to be admitted pro hac vice)*
BURNS CHAREST LLP
365 Canal Street, Suite 1170
New Orleans, Louisiana 70130
Telephone: (504) 799-2845
knelson@burnscharest.com

Monica Miller
Charles J. LaDuca
Brendan Thompson
Alex Warren
CUNEO GILBERT & LADUCA, LLP
4725 Wisconsin Avenue NW, Suite 200
Washington, DC 20016
Telephone: (202) 789-3960
monica@cuneolaw.com
charles@cuneolaw.com
brendant@cuneolaw.com
awarren@cuneolaw.com

Don Barrett
BARRETT LAW GROUP, P.A.
404 Court Square North
Lexington, MS 39095
Telephone: (662) 834-9168
donbarrettpa@gmail.com

William M. Audet
Ling Y. Kuang
AUDET & PARTNERS, LLP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 568-2555
waudet@audetlaw.com
lkuang@audetlaw.com

Counsel for Named Plaintiff and the Class